CCNA Study Guide

Alexander

June 9, 2024

1. Network Fundamentals (20%)
2. Network Access (20%)
3. IP Connectivity (25%)
4. IP Services (10%)
5. Security Fundamentals (15%)
6. Automation and Programmability (10%)

Network Fundamentals

- Explain the role and function of network components

  Routers forward packets between computer networks (LANs and WANs), and use IP addresses to determine where the packet should go.

  L2 switches forward data frames within the same network segment using MAC addresses. L3 switches can perform switching functions in addition to routing functions.

  Firewalls sit in the path that packets take through the network. They permit/deny traffic much like an ACL would do on a router. Firewalls are capable of watching application-layer flows with AVC, performing webpage verification on URIs, and retaining state. IPSs can compare packet flows to exploit signatures, log events, and can discard/redirct packets.

  An AP serves as a single point of contact for every device that wants to use a BSS. An AP uses a unique BSSID that is based on the AP's own radio MAC address. APs are often connected to a DS that uplinks to a wired network.

- Describe characteristics of network topology architectures
- Compare physical interface and cabling types

- Identify interface and cable issues (collisions, error, mismatch duplex, and/or speed)
- Compare TCP to UDP
- Configure and verify IPv4 addressing and subnetting

  ```
  Router(config-if)# ip address <ip_address> <subnet_mask>
  ```

  ```
  Router# show ip interface brief
  ```

- Describe private IPv4 addressing
- Configure and verify IPv6 address types

  ```
  Router(config-if)# ipv6 address <IPv6_address>/<prefix_length>
  ```

  ```
  Router# show ipv6 interface brief
  ```

- Describe IPv6 addressing and prefix
- Verify IP parameters for Client OS
- Describe wireless principles
- Explain virtualization fundamentals (server virtualization, containers, and VRFs)
- Describe switching concepts

Network Access

- Configure and verify VLANs (normal range 0-1005) spanning multiple switches

  ```
  Switch(config)# vlan <vlan-id>
  Switch(config-if)# switchport mode access
  Switch(config-if)# switchport access vlan <vlan-id>
  ```

  ```
  Switch# show vlan
  ```

- Configure and verify interswitch connectivity

  ```
  Switch(config-if)# switchport mode trunk
  Switch(config-if)# switchport trunk allowed vlan <10,20,30>
  Switch(config-if)# switchport tunk encapsulation <dot1q/isl>
  Switch(config-if)# switchport trunk native vlan <vlan-id>
  ```

Switch# show interface trunk
Switch# show interface interface_type interface_number

- Configure and verify L2 discovery protocols (CDP/LLDP)

  Switch(config)# <cdp/lldp>run Switch# show <cdp/lldp>neighbors

- Configure and verify (L2/L3) EtherChannel (LACP)

  Manual Switch(config-if-range)# channel-group 1 mode on

  Dynamic Switch(config-if-range)# channel-group 1 mode <desirable/auto>(PAgP) Switch(config-if-range)# channel-group 1 mode <active/passive>(LACP)

  you can load balance by source and/or destination MACs, IPs, or ports Switch(config)# port-channel load-balance method

  Etherchannels are dependent on many other items: speed, duplex, operational mode, VLANs, STP Switch# show etherchannel summary Switch# show interfaces status

  L3 Etherchannel configuration is similar to L2 configuration however: 1. each physical port need to be a routed port (no switchport command) 2. the actually channel needs to be a routed port with an IP and mask

- Interpret basic operations of Rapid PVST+ Spanning Tree Protocol
- Describe Cisco Wireless Architectures and AP modes
- Describe physical infrastructure connections of WLAN components (AP, WLC, access/trunk ports, and LAG)
- Describe network device management access (Telnet, SSH, HTTP, HTTPS, console, TACACS+/RADIUS, and cloud managed)
- Interpret the wireless LAN GUI configuration for client connectivity, such as WLAN creation, security settings, QoS profiles, and advanced settings

IP Connectivity

- Interpret the compnents of routing table
- Determine how a router makes a forwarding decision by default
- Configure and verify IPv4 and IPv6 static routing
- Configure and verify single area OSPFv2

- Describe the purpose, functions, and concepts of first hop redundancy protocols

IP Services

- Configure and verify inside source NAT using static and pools
- Configure and verify NTP operating in a client and server mode
- Explain the role of DHCP and DNS within the network
- Explain the function of SNMP in network operations
- Describe the use of syslog features including facilities and levels
- Configure and verify DHCP client and relay
- Explain the forwarding per-hop behavior (PHB) for QoS, such as classification, marking, queuing, congestion, policing, and shaping
- Configure network devices for remote access using SSH
- Describe the capabilities and functions of TFTP/FTP in the network

Security Fundamentals

- Define key security concepts (threats, vulnerabilities, exploits, and mitigation techniques)
- Describe security program elements (user awareness, training, and physical access control)
- Configure and verify device access control using local passwords
- Describe security password policies elements, such as management, complexity, and password alternatives (multifactor authentication, certificates, and biometrics)
- Describe IPsec remote access and site-to-site VPNs
- Configure and verify access control lists
- Configure and verify Layer 2 security features (DHCP snooping, dynamic ARP inspection, and port security)
- Compare authentication, authorization, and accounting concepts
- Describe wireless security protocols (WPA, WPA2, and WPA3)
- Configure and verify WLAN within the GUI using WPA2 PSK

Automation and Programmability

- Explain how automation impacts network management
- Compare traditional networks with controller-based networking
- Describe controller-based, software defined architecture (overlay, underlay, and fabric)
- Explain AI (generative and predictive) and machine learning in network operations
- Describe characteristics of REST-based APIs (authentication types, CRUD, HTTP verbs, and data encoding)
- Recognize the capabilities of configuration management mechanisms, such as Ansible and Terraform
- Recognize components of JSON-encoded data